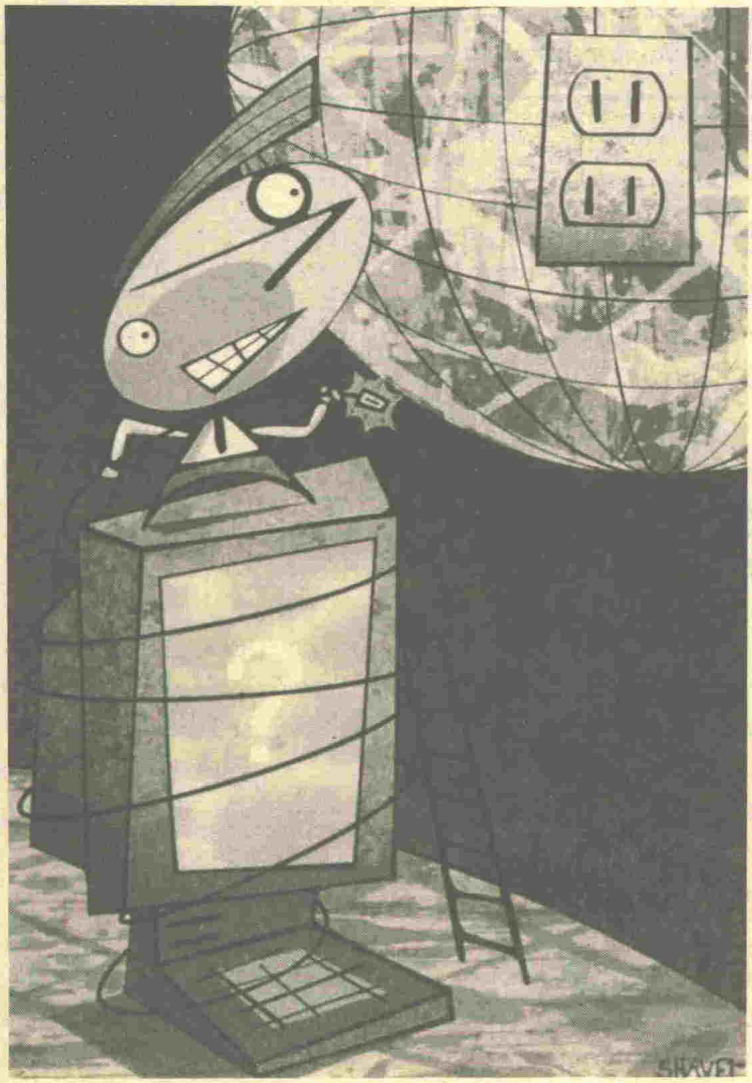
ยืน ภู่วรวรรณ

ICMP โปรโตคอลช่วย TCP/IP

ICMP เป็นเพียงโปรโตคอลที่ช่วยให้ระบบทำงานดียิ่งขึ้น เข้ามาช่วยแก้ปัญหาที่เกิดจากการทำงานปกติของระดับ 3 คือ IP



ผู้ใช้อินเทอร์เน็ตคงมีความประหลาดใจและเห็นถึงความมหัศจรรย์ของเครือข่ายขนาดใหญ่ที่เชื่อมโยงต่อถึงกันได้ทั่วโลก การพัฒนาและออกแบบโปรโตคอลสำหรับเครือข่ายและการเชื่อมโยงที่สำคัญคือโปรโตคอล TCP/IP การที่เรียกว่า TCP/IP นั้นอาจเรียกเพราะเป็นโปรโตคอลหลัก เพราะการกำหนดเส้นทางและการเชื่อมโยงระหว่างเครื่องคอมพิวเตอร์ใช้โปรโตคอล IP โดยมีส่วนของการทำงานอยู่ระดับ 3 เหนือจาก LAN หรือ WAN ที่ทำงานในระดับ 1 กับ 2 ตามที่ได้เคยมีบทความในวารสารไมโคร ฯ หลายครั้งที่เกี่ยวกับ TCP/IP ซึ่งแสดงให้เห็นว่าในระดับ 4 การทำงานจริง ๆ แล้วมีการใช้ UDP และ TCP ซึ่งขึ้นกับการประยุกต์ใช้งาน ดังนั้นหากจะเรียกให้ถูกต้องน่าจะเป็น TCP หรือ UDP/IP แต่เนื่องจาก TCP/IP เป็นคำที่คุ้นเคยและติดปากจึงใช้คำนี้

ในการหาเส้นทางและตรวจสอบเส้นทางการเชื่อมโยงบนเครือข่ายนั้นมีโปรโตคอลย่อยที่ทำงานอยู่อีกหลายโปรโตคอล เช่น ARP และ RARP ที่ทำหน้าที่เชื่อมโยงการทำงานระหว่างระดับ 3 กับ 2 ให้แน่นแฟ้นยิ่งขึ้น

สำหรับในระดับ 3 เป็นระดับของการหาเส้นทางซึ่งเป็นกรรมวิธีที่สำคัญ บนโปรโตคอลที่ใช้ในอินเทอร์เน็ตมีโปรโตคอล ICMP-Internet Control Message Protocol ซึ่งเป็นโปรโตคอลที่สำคัญควบคุมการทำงานอยู่

เพื่อให้เข้าใจเกี่ยวกับ ICMP ได้ดียิ่งขึ้น ผู้เขียนขอแนะนำให้มีการทบทวนเรื่อง TCP/IP ที่เคยมีหลายท่านได้เขียนไว้แล้วในวารสารไมโครฯ เล่มก่อน ๆ

ระดับการเกี่ยวโยงของโปรโตคอลต่าง ๆ ที่ใช้งานร่วมกันแสดงดังรูปที่ 1

จากโครงสร้างความสัมพันธ์นี้เห็นได้ชัดว่า ICMP อยู่ในระดับ 3 ซึ่งเป็นระดับเน็ตเวอร์ก เป็นโปรโตคอลที่สำคัญที่ช่วยในการหาเส้นทางของการเชื่อมโยงเครือข่าย

รู้จักกันดีด้วยคำสั่ง ping

เมื่อผู้ใช้งานบนอินเทอร์เน็ตอยากรู้ว่าโฮสต์ที่ตนเองจะติดต่อมีตัวตนและเชื่อมโยงเส้นทางไปถึงได้หรือไม่ เรามีคำสั่งง่าย ๆ คำสั่งหนึ่งคือคำสั่ง ping คำสั่ง ping ใช้โปรโตคอล ICMP เพื่อส่งไปยังปลายทางแล้วส่งคำตอบกลับมา ลองดูตัวอย่าง

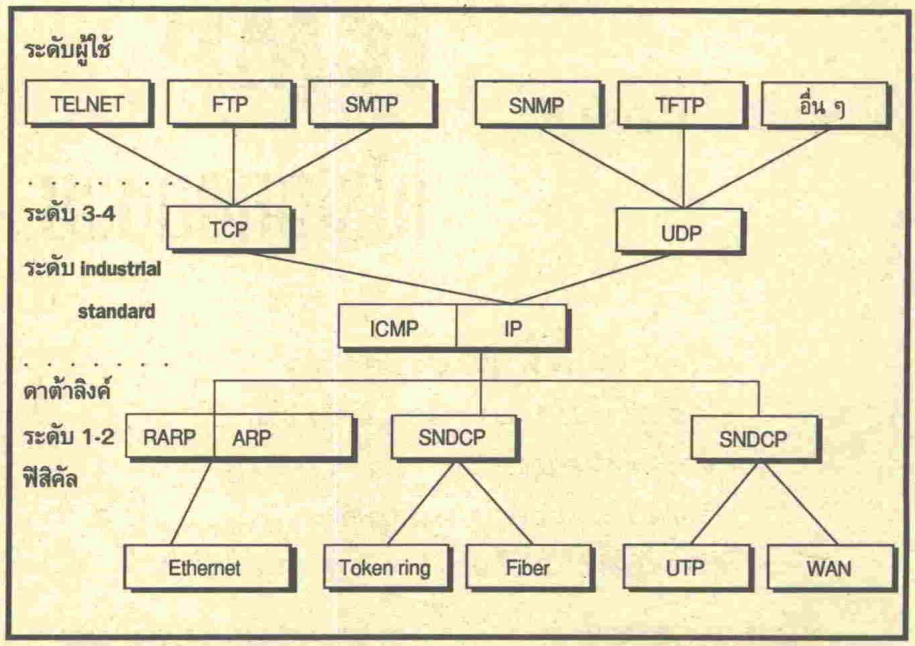
```
nontri% ping nwg.nectec.or.th
nwg.nectec.or.th is alive
nontri%
```

กรณีของการ ping ด้วยพารามิเตอร์ที่บอกจำนวนไบต์และจำนวนแพคเก็ต แสดงดังรูปที่ 2

คำสั่งแรกใช้ ping ส่งโปรโตคอล ICMP ไปถาม ส่วนคำสั่งที่สองมีการกำหนดให้ส่งข้อความไปถาม 14 ข้อความ ซึ่งแต่ละข้อความมีความยาว 64 ไบต์ ผลที่ได้เป็นการบอกข้อมูลว่าแพคเก็ต ICMP ใช้เวลาเท่าไร และมีจำนวนแพคเก็ตที่สูญหายหรือไปไม่ถึงอยู่เท่าไร

ICMP คืออะไร

IP เป็นโปรโตคอลที่ค่อนข้างเรียบง่าย มีโครงสร้างที่ได้รับการออกแบบมาอย่างดี ใช้งานได้อย่างยอดเยี่ยม การใช้งาน IP เพื่อเชื่อมโยงเป็นไปอย่างมีประสิทธิภาพและใช้ทรัพยากรที่ค่อนข้างจำกัด แต่ก็ยังมีปัญหาบางประการ เช่น เมื่อเราเตอร์ทำงานผิดพลาดหรือมีบางแพคเก็ตที่ไม่สามารถนำส่งได้ หรือช่วงเวลาที่ทำงานเกินขอบเขตที่ตั้งไว้ อะไรจะเป็นตัวคอยบอกหรือเตือนให้ทราบว่าข้อมูลข่าวสารที่จัดส่งนี้ไปไม่ถึงปลายทาง หรือหากบางเราเตอร์มีปัญหาในการนำส่งการส่งข้อมูลเตือนกลับไปยังโฮสต์จะทำได้อย่างไร เพื่อให้การทำงานในเรื่องการสร้างเครือข่ายเส้นทางหรือตอบสนองปัญหาที่ต้องการจึงต้องมีโปรโตคอลพิเศษ



รูปที่ 1 ความสัมพันธ์ของโปรโตคอลระดับต่าง ๆ

```
nontri% ping -s nwg.nectec.or.th 64 14
PING nwg.nectec.or.th: 64 data bytes
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=0 . time=460  . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=1 . time=1038 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=2 . time=1402 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=3 . time=1162 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=4 . time=1855 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=5 . time=1080 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=7 . time=1606 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=8 . time=1006 . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=9 . time=729  . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=10.time=985  . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=11.time=772  . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=12.time=288  . ms
72 bytes from nwg.nectec.or.th (192.150.251.31) : icmp_seq=13.time=587  . ms
--nwg.nectec.or.th PING Statistics--
14 packets transmitted, 13 packets received, 7% packet loss
round-trip (ms) min/avg/max = 288/997/1855
nontri%
```

รูปที่ 2

ICMP เป็นโปรโตคอลที่เข้ามาช่วยเสริมแก้ปัญหาระบบดังกล่าวนี้ ICMP เป็นโปรโตคอลที่ช่วยเหลือระบบให้ทำงานได้อย่างมีประสิทธิภาพ ช่วยทำให้การดูแลเครือข่ายหรือการแสดงสถานะของเครือข่ายที่โหนดต่าง ๆ เป็นไปอย่างถูกต้องและแจ้งสถานะของตนเองได้

ฟังก์ชันการทำงานของ ICMP จึงเป็นส่วนหนึ่งของ IP โฮสต์ทุกโฮสต์ และเราเตอร์ต้องสร้าง ICMP เพื่อใช้ในการตรวจสอบสถานะหรือติดต่อแสดงสถานะของเครือข่าย

ICMP เป็นข้อมูลและบรรจุใน IP แพคเก็ต โดยมีส่วนหัวเป็นส่วนของ IP โครงสร้างของ ICMP จึงมีลักษณะดังรูปที่ 3

ส่วนหัวของ IP เป็นส่วนที่หาอ่านได้จากวารสารไมโครเล่มก่อน ๆ ซึ่งมีบทความเกี่ยวกับ TCP/IP มาแล้วหลายครั้ง ในส่วนหัวนี้มีข้อมูลในฟิลด์ Type of Service เป็น 0 และรหัสโปรโตคอลได้รับการเซตให้มีค่าเป็น 1 ดังนั้นถ้าพิจารณาให้ดีก็จะเห็นได้ว่าส่วนของข้อความที่เป็น ICMP จะเป็นข้อมูลของแพคเก็ต IP เป็นการทำงานเสมือนการใช้แพคเก็ต IP

รูปที่ 3 แสดงแพคเก็ตของ ICMP ที่ใช้ส่วนหัวเป็น IP

ICMP ใช้เป็นสัญญาณบ่งบอกข้อผิดพลาด

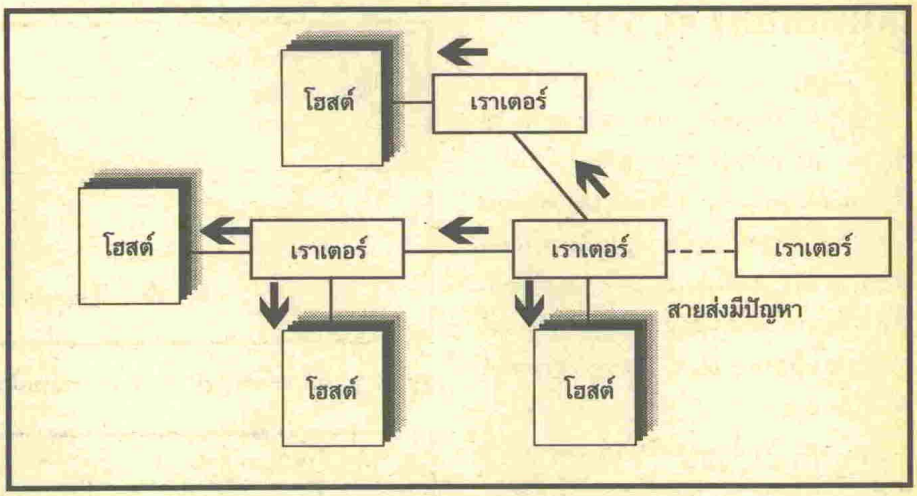
ลองนึกดูว่าเมื่อมีการส่งข้อมูลด้วยแพคเก็ต IP จากโฮสต์หนึ่งไปอีกโฮสต์หนึ่งผ่านเราเตอร์หลาย ๆ ตัว ผลที่เกิดขึ้นอย่างหนึ่งคือเมื่อสายเชื่อมโยงช่วงใดช่วงหนึ่งขาด เราเตอร์อาจทำการดึงข้อมูลออกจากระบบและไม่นำส่งต่อ หรือบางครั้งข้อมูลที่ส่งมีการแบ่งแยกเป็นก้อนเล็ก ๆ และรู้แน่ว่าข้อมูลไม่สามารถดำเนินการได้สำเร็จ การรายงานแจ้งกลับจึงเป็นเรื่องสำคัญที่ต้องดำเนินการ

หากมีการดำเนินการส่งข้อมูลออกจากระบบ เราเตอร์หรืออุปกรณ์ที่ดำเนินการจะต้องส่ง ICMP กลับไปบอก ดังตัวอย่างในรูปที่ 4

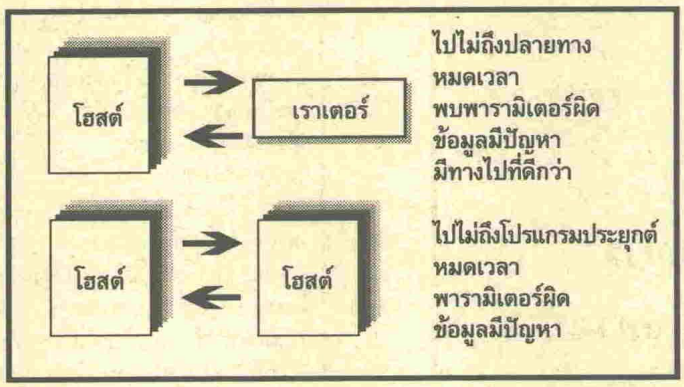
การสร้างระบบจึงต้องทำให้มีการแจ้งปัญหาที่เกิดขึ้นอย่างทันทีทันใดและรวดเร็วเพื่อลดปัญหาที่มีข้อมูลส่งตามมาอีกจำนวนมาก การแจ้งปัญหาจึงไม่เกี่ยวกับระบบการจัดการหรือศูนย์กลางการดูแลเครือข่าย เพราะเครือข่ายที่ต่ออยู่เชื่อมโยงกันเป็นเครือข่ายขนาดใหญ่มาก

การแจ้งกลับด้วย ICMP ก็เป็นส่วนหนึ่งที่ทำให้เกิดปริมาณข้อมูลข่าวสารในเครือข่ายเพิ่มขึ้น แต่อย่างไรก็ดี การดำเนินการในลักษณะนี้จะเน้นการตอบกลับไปยังแหล่งที่จะติดต่อ

การดำเนินการดูแลเครือข่ายมีโปรโตคอล SNMP ช่วยจัดการ ซึ่งเป็นโปรโตคอลพิเศษสำหรับการดูแลเครือข่ายโดยเฉพาะ



รูปที่ 4 การส่ง ICMP ตอบกลับไปยังสถานีต้นทาง



รูปที่ 5 ลักษณะการแจ้งเหตุด้วย ICMP

ชนิดของข้อความแจ้งเหตุผิดพลาด

เมื่อมีปัญหาหรือเหตุผิดพลาดเกิดขึ้นในเครือข่าย จะมีการตอบกลับเป็นรหัสสำหรับการแจ้งข้อผิดพลาด โดยใช้โฮสต์ปลายทางหรือเราเตอร์ ข้อผิดพลาดที่เกิดขึ้นพอสรุปเป็นรูปภาพได้ดังรูปที่ 5

ปัญหาที่ใช้ ICMP แจ้งเหตุคือ

- แพคเก็ต (datagram) ไม่สามารถไปถึงปลายทางได้
- เวลา (time to live) ซึ่งได้กำหนดไว้ในแพคเก็ตหมดเวลา
- ส่วนหัวของ IP มีลักษณะผิดปกติ
- เราเตอร์หรือโฮสต์ปลายทาง congest
- ตัวโฮสต์กำหนดเส้นทางไปยังเราเตอร์ผิด
- เวลาในการรวมข้อมูลหมด

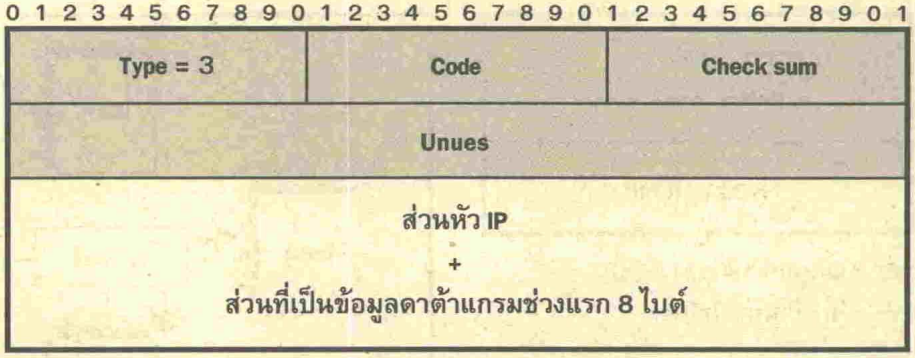
โปรโตคอลของ ICMP เป็นตัวกำหนดให้มีการส่งข้อความรายงานข้อผิดพลาด โดยมีการรายงานกลับไปให้ส่วนที่จะนำไปใช้ประโยชน์ต่อไป เพื่อให้โปรแกรมรับรู้และแก้ปัญหาได้ การคาดหวังที่จะให้ ICMP รายงานข้อผิดพลาดเป็นเรื่องดี แต่ไม่ได้หมายความว่า ICMP ต้องรวบรวมข้อผิดพลาดทุกเรื่อง และเราก็ไม่ต้องการเห็นการรายงานวิ่งมาบนเครือข่ายจนทำให้มีข้อมูลเหล่านี้วิ่งมามากมายเต็มไปหมด ICMP จะไม่รายงานข้อผิดพลาดจากปัญหาต่อไปนี้

- ข้อความ ICMP ที่ได้รับหรือ ICMP ที่ใช้กำหนดเส้นทาง
- ดาต้าแกรมที่ใช้ในการกระจายในเครือข่าย
- การทำ fragment ดาต้าแกรมที่ไม่ใช่อันแรก

รูปแบบของ ICMP

ข้อความทั้งหมดของ ICMP จะได้รับการบรรจุในฟิลด์ข้อมูลของดาต้าแกรม IP ข้อความ ICMP ทุก ๆ รูปแบบเริ่มด้วยฟิลด์ 3 ฟิลด์ ฟิลด์แรกเป็นฟิลด์ชนิดข้อความ (message type) ฟิลด์ที่สองเป็นรหัส (code) และฟิลด์ที่สามคือฟิลด์ตรวจสอบผลบวก (check sum) ส่วนรูปแบบที่เหลือนอกเหนือจากสามฟิลด์นี้จะขึ้นกับชนิดของ ICMP ที่กำหนดในฟิลด์ message type

ข้อความที่แสดงว่าเป็นข้อผิดพลาดที่ ICMP ใช้รายงานจะประกอบด้วยส่วนหัวของ IP และข้อมูล 8 ไบต์ของดาต้าแกรมที่เป็นต้นเหตุให้เกิดข้อผิดพลาด ข้อมูลเหล่านี้เป็นพื้นฐานสำหรับการแก้ปัญหา เพราะข้อมูล 8 ไบต์ในส่วนที่ใส่เข้ามาจะเป็นส่วนหัวของโปรโตคอล TCP, UDP ในระดับ 4



รูปที่ 6 รูปแบบของ ICMP ที่รายงานกรณีไปถึงปลายทางไม่ได้

ข้อความที่บอกการไปไม่ถึงสถานีปลายทาง

มีหลายกรณีที่เมื่อส่งดาต้าแกรม IP ไปแล้วไม่สามารถไปถึงปลายทางได้ สาเหตุที่สำคัญ เช่น สายเชื่อมโยงมีปัญหา เราเตอร์ดำเนินการเชื่อมต่อไปปลายทางไม่ได้ หรือมีการดำเนินการกำหนดเส้นทางซึ่งหมายถึงเป็นลูปหรือย้อนกลับไปต้นทาง หรือเครื่องโฮสต์ปลายทางไม่มีเนื่องจากการไม่เปิด เครื่องเสีย หรืออยู่ระหว่างการซ่อมบำรุง

ปัจจุบันนี้มีการพัฒนาเราเตอร์ให้มีขีดความสามารถสูงมาก โดยเฉพาะมีเรื่องการดูแลรักษาความปลอดภัย เราเตอร์มีขีดความสามารถที่จะรับโปรแกรมการทำงานเฉพาะได้หลายอย่าง เช่น เลือกเส้นทางหรือปฏิเสธการส่งข้อมูลไปยังบางเส้นทางหรือบางโฮสต์ได้ ผู้โปรแกรมเราเตอร์สามารถโปรแกรมให้ป้องกันการเรียกเข้าหาโฮสต์ใด หรือป้องกันไม่ให้โฮสต์ใดเรียกเข้าหา เมื่อเป็นเช่นนี้จะมีข้อมูลบางดาต้าแกรมที่ถูกปฏิเสธไม่ให้เดินทางต่อ การดูแลและการจัดการเครือข่ายจึงมีลักษณะเฉพาะมากขึ้น

รหัส	ความหมาย
0	ไปไม่ถึงเครือข่าย
1	ไปไม่ถึงโฮสต์
2	โปรโตคอลปลายทางไปไม่ถึง
3	ไปไม่ถึงพอร์ต
4	มีความต้องการรวมข้อมูลหลายแพคเก็ต แต่ไม่สามารถกระทำได้ โดยมีแฟลกเป็นตัวบ่งบอกไว้
5	เส้นทางต้นทางผิดพลาด
6	ไม่รู้จักเครือข่ายปลายทาง
7	ไม่รู้จักกับโฮสต์ปลายทาง
8	โฮสต์ต้นทางถูกแยกตัวออก
9	การสื่อสารที่เครือข่ายปลายทางได้รับการจัดการป้องกันไว้
10	โฮสต์ที่ปลายทางได้รับการจัดการป้องกันไว้
11	ไปไม่ถึงเครือข่าย สำหรับการบริการงานบางอย่าง
12	ไปไม่ถึงโฮสต์ สำหรับการบริการงานบางอย่าง

ตารางที่ 1 รหัสของ ICMP กรณี type 3

เมื่อเราเตอร์ปฏิเสธการนำส่งข้อมูล (ดาต้าแกรม) จึงต้องมีข้อความส่งกลับเพื่อบอกให้รู้ว่านำส่งต่อไปไม่ได้ หรือไปไม่ถึงที่หมาย เพื่อว่าจะได้ให้โฮสต์ต้นทางได้รับทราบ

ฟอร์แมตของ ICMP ที่ตอบกลับเพื่อบอกให้รู้ว่าการเดินทางของข้อมูล (ดาต้าแกรม) ไปไม่ถึงปลายทาง การใช้ ICMP ในกรณีนี้จะใช้ Type = 3 และให้รหัสเป็นตัวบอกความหมายรหัสอยู่ในฟิลด์ code เป็นดังตารางที่ 1

ICMP–แสดงการใช้เวลาเกินกำหนด

การส่งข้อมูล (ดาต้าแกรม) ไปในเครือข่ายมีการกำหนด time to live เป็นพารามิเตอร์หนึ่งใน IP เมื่อข้อมูล IP ผ่านไปแต่ละช่วงจะมีการลดค่า time to live ลง และหากค่าเป็นศูนย์ก็หมายถึงหมดเวลาแล้ว เราเตอร์จะทำหน้าที่เก็บข้อมูลส่วนนี้ออกไป

กรณีการหมดเวลาอีกประการหนึ่งคือการรวมข้อมูล เพราะข้อมูลที่ส่งอาจมีข้อมูลเป็นกลุ่มหรือแพคเก็ตต้นทางขนาดใหญ่ และเมื่อเปลี่ยนโปรโตคอลก็มีการแบ่งแยก และต้องมีการรวมกันใหม่ การรวมข้อมูลนี้เราเตอร์รับข้อมูลส่วนแรกแล้วจะต้องรอข้อมูลส่วนที่ตามมา ซึ่งจะต้องนำมารวมกัน เช่น ด้านหนึ่งของเราเตอร์เป็นอีเธอร์เน็ต อีกด้านหนึ่งเป็นโทเก้นริง เมื่อได้ข้อมูลอีเธอร์เน็ตมาแต่ละ IP จะยังไม่สามารถส่งกลับออกทางโทเก้นริง อาจต้องรอข้อมูลแพคเก็ตต่อมา หากรอนานไปข้อมูลยังไม่มา ก็มีการกำหนดเวลาบอกถึงการหมดเวลา

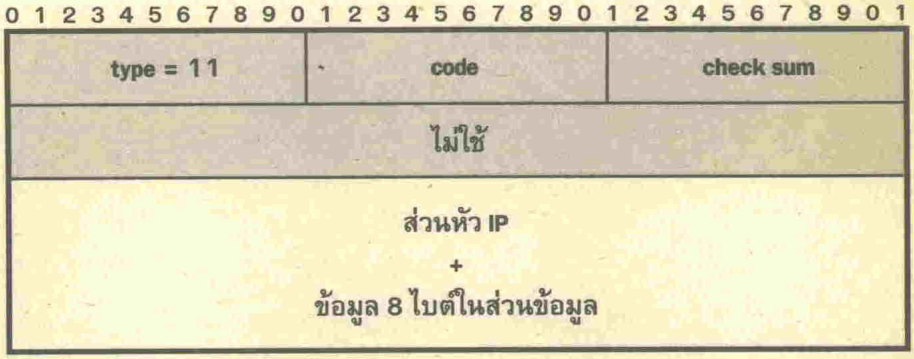
รูปแบบข้อมูล ICMP แสดงการใช้แล้วเกินกำหนด แสดงดังรูปที่ 7

ในกรณีนี้ใช้ type = 11 โดยที่รหัสมีความหมายดังนี้

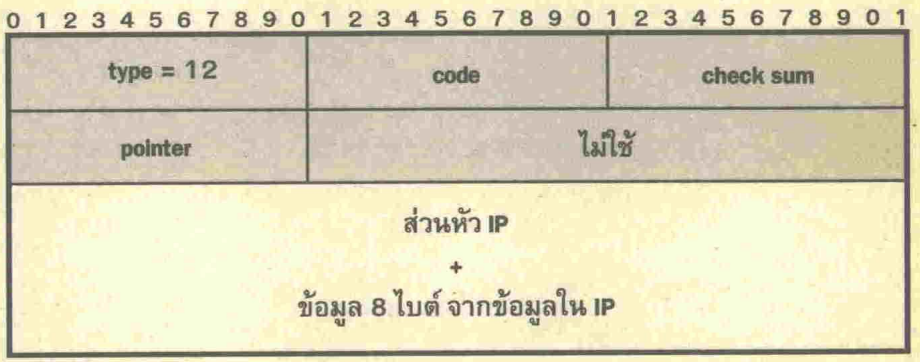
0 หมายถึง เวลาที่ใช้เกินกำหนด

1 หมายถึง การรวมข้อมูลเกินกำหนด

อย่าลืมว่าการรวมข้อมูลในกรณีนี้คือการ flagment ซึ่งคือการแบ่งแพคเก็ตในระดับ 2 ให้เป็นระดับ 3 (IP) ที่มีขนาดไม่เท่ากัน



รูปที่ 7 ICMP แสดงการใช้เวลาเกินกำหนด



รูปที่ 8 ICMP แสดงปัญหาจากพารามิเตอร์ผิดพลาด

ICMP แสดงปัญหาพารามิเตอร์ผิดพลาด

ในการรับส่งข้อมูลดาต้าแกรม (IP แพคเก็ต) แต่ละแพคเก็ตมีส่วนหัวของ IP เป็นตัวบอกรายละเอียดบางอย่าง บางครั้งส่วนหัว IP มีการผิดพลาด ทำให้แปลความหมายของข้อมูลใน IP แพคเก็ตนั้นได้ หากเราเตอร์หรืออุปกรณ์รับส่งข้อมูลพบว่าส่วนหัวของ IP ผิดพลาดก็ควรจะต้องรายงานข้อผิดพลาดกลับไป รหัส ICMP ในส่วนของ type มีค่าเป็น 12 ดังรูปที่ 8

ส่วนรหัสที่ใช้แสดงความหมายมีดังนี้

0 หมายถึง ค่าจำนวนใน pointer เป็นตัวชี้ฟิลด์ที่ผิดพลาด

1 หมายถึง ในส่วนของ option ผิดพลาด (ส่วนนี้ได้รับการนำมาใช้ในเรื่องทางทหาร)

โดยปกติหัวของ IP มีการกำหนดไว้ชัดเจน (หาดูเพิ่มเติมจากบทความ TCP/IP ในวารสารไมโครฯ ฉบับก่อน ๆ) ส่วนฟิลด์ใน option เป็นส่วนที่มีปัญหามาก และอาจมีข้อผิดพลาดได้

ICMP บอกต้นทางหยุดส่ง

ขบวนการโปรโตคอล IP เป็นขบวนการที่ง่ายและดูตรงไปตรงมา การทำงานทั้งของโฮสต์หรือเราเตอร์ทำงานอย่างรวดเร็วและทันที ทันใดที่มีข้อมูลวิ่งเข้ามา อย่างไรก็ดี ข้อมูลที่เดินทางก็อาจมีการสะดุดหรือมีปัญหาได้

ลองนึกดูว่าหากมีการส่งข้อมูลในระดับ 4 เช่น UDP ไปยังเซอร์ฟเวอร์ที่ทำงานได้ช้า อาจทำให้ข้อมูลไปที่เซอร์ฟเวอร์อย่างมากมาย จนเกิดโอเวอร์โฟลว์ขึ้นที่เซอร์ฟเวอร์ได้ หรือบางครั้งกรณีของเราเตอร์มีบัฟเฟอร์ที่เป็นหน่วยความจำอยู่จำกัด และเราเตอร์รับข้อมูลจากทางเข้าด้วยความเร็วสูงมาก เช่น เป็นอีเธอร์เน็ตหลายเซกเมนต์ ต่อออกไปยังปลายทางที่เป็น WAN พอร์ตความเร็วต่ำ อาจทำให้เราเตอร์ทำงานด้วยบัฟเฟอร์ขนาดเล็กไม่ได้ จึงจำเป็นต้องส่ง ICMP ไปบอกต้นทางให้หยุดส่งมาก่อน เพื่อลดปัญหาที่อาจจะเกิดจากการทำงานผิดพลาดและต้องการให้ทำใหม่ซ้ำแล้วซ้ำเล่า ยิ่งเป็นการสร้างปัญหายิ่งขึ้น

การที่ข้อมูลดาต้าแกรมจำนวนมากเข้ามาและจะต้องถูกทิ้งไป ยิ่งเป็นข้อเสียของระบบโดยรวม เพราะเมื่อต้นทางส่งข้อมูลถึงปลายทางไม่ได้หมด ก็จะต้องส่งซ้ำ การหยุดปัญหานี้จึงต้องใช้ ICMP ช่วย

รูปแบบของ ICMP ในกรณีที่เป็นดังรูปที่ 9

ส่วนของ ICMP รูปแบบนี้จะได้รับการส่งไปยังต้นทางโดยส่งไปยังระดับบนคือ TCP หรือ UDP ในส่วนของโปรแกรมประยุกต์ ให้โปรแกรมประยุกต์แก้ปัญหาในส่วนนี้ด้วย และเพื่อให้ช่วยดำเนินการแก้ปัญหาโดยผู้เขียนโปรแกรมจะต้องคำนึงถึง แต่สิ่งที่จะต้องพิจารณาในระบบรวมคือ

"เมื่อไรเราเตอร์หรือโฮสต์จึงจะส่ง ICMP ชนิดนี้ไปบอกแหล่งส่งข้อมูล และอุปกรณ์ประเภทใดที่เป็นต้นทางสำหรับการที่จะส่ง ICMP ไป"

กรรมวิธีการทำงานจึงต้องเป็นไปอย่างชาญฉลาด กล่าวคือ ในกรณีที่มีการเกิดโอเวอร์โฟลว์ของข้อมูล บางครั้งก็ไม่รู้ว่ามาจากที่ใด เพราะข้อมูลถูกยกเลิกไปเอง การส่งกลับไปบอกจึงทำไม่ได้ การส่งกลับไปบอกจึงเป็นวิธีการที่จะลดจำนวนดาต้าแกรมที่กำลังวิ่งมาอย่างมากให้ลดลง และเมื่อโหลดว่างแล้วจึงให้ส่งมาอีก วิธีนี้จะทำให้ต้นทางหยุดส่งชั่วขณะหนึ่ง

ICMP–redirect

ในเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมโยงกันระหว่างเราเตอร์หลาย ๆ ตัว และมีเส้นทางการเชื่อมโยงได้หลายทาง การส่งดาต้าแกรม

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
Type = 4	Code	Check sum
ไม่ใช้		
ข้อมูลส่วนหัว IP + ข้อมูลใน IP 8 ไบต์		

รูปที่ 9 ICMP ที่ส่งบอกให้ต้นทางหยุดส่ง

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
Type = 5	Code	Check sum
แอดเดรสของเราเตอร์ที่ใช้		
ส่วนหัวของ IP + ข้อมูล 8 ไบต์ในแพคเก็ต IP		

รูปที่ 10

จากต้นทางไปยังปลายทางผ่านเราเตอร์หลายตัวอาจมีได้หลายทางเลือก การกำหนดเส้นทางบนเราเตอร์มีตารางการส่งที่เรียกว่า ตารางเราติ้ง อย่างไรก็ดี เส้นทางที่กำหนดถ้ากำหนดแบบตายตัวก็จะทำให้ไม่เกิดประสิทธิภาพที่ดีได้ เพราะทางเลือกอื่นอาจทำไม่ได้ ดังนั้นจึงมีความคิดที่จะให้มีการหาเส้นทางที่ดีที่สุดหรือการสร้างตารางเราติ้งได้เองอย่างอัตโนมัติ วิธีการหนึ่งคือให้มีการส่ง ICMP กลับไปยังโฮสต์และให้โฮสต์พิจารณาว่าเส้นทางที่ไปยังปลายทางเป็นอย่างไร จะมีการปรับเปลี่ยนเพื่อให้เส้นทางสั้นกว่านี้หรือไม่ เป็นการกระทำแบบไดนามิกได้

ICMP ส่วนนี้จึงทำให้การจัดการเครือข่ายเป็นไปเองโดยไม่ต้องคอยกำหนดด้วยมือ โฮสต์จะได้รับการกำหนดให้มีฟังก์ชันที่ทำงานกำหนดเส้นทางแบบเริ่มต้นอย่างใดอย่างหนึ่งก่อนแล้วจะเรียนรู้ โดยได้รับข้อมูลจากเราเตอร์ตัวอื่น ๆ

รหัสของ ICMP redirect เป็นดังรูปที่ 10

รหัสที่ใช้ประกอบด้วย

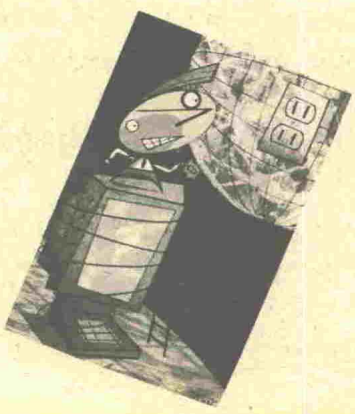
0 หมายถึง การส่งข้อความ redirect สำหรับเครือข่าย

1 หมายถึง การส่งข้อความ redirect สำหรับโฮสต์

2 หมายถึง การส่งข้อความ redirect สำหรับชนิดของการบริการของเครือข่าย

3 หมายถึง การส่งข้อความ redirect สำหรับชนิดของการบริการของโฮสต์

เราเตอร์จะมีตารางการกำหนดเส้นทางซึ่งเก็บข้อมูลของโฮสต์หรือของเครือข่ายไว้เพื่อบอกว่าจะให้มีการกำหนดเส้นทางจากต้นทางไปปลายทางผ่านเราเตอร์อย่างไร



ICMP ก็เป็นคำถามได้

จากที่กล่าวมาในตอนแรกนี้ ICMP เป็นแบบการให้ข้อมูลหรือการแจ้งกลับ แต่การทำงานของเครือข่ายบางครั้งก็ต้องมีการส่งคำถามไปถามด้วย เพื่อให้ผู้ได้รับคำถามส่งคำตอบมา คำถามที่จำเป็นและต้องการในระบบมากมีหลายคำถาม เช่น โฮสต์ A เปิดอยู่หรือเปล่า? เราเตอร์ B กำลังทำงานหรือไม่? ถ้าให้ข้อมูลเดินทางไปยัง Z และกลับมาจะใช้เวลาเท่าไร? แอดเดรสมาสก์ของเราเตอร์มีหมายเลขอย่างไร?

คำถาม ICMP จึงเป็นเรื่องสำคัญ เพราะระบบจะต้องมีการรับรู้ข้อมูลและปรับแต่งให้ทำงานอย่างมีประสิทธิภาพ คำถาม ICMP จึงประกอบด้วย

- คุณยังอยู่ดีหรือ (Are you alive?) เป็นคำถามที่โฮสต์หรือเราเตอร์สอบถามกันและมีการให้คำตอบ

- การประทับเวลา โดยมีคำถามที่จะส่งไปยังปลายทางและให้แต่ละขั้นมีการประทับเวลา (โดยลดค่าลง) เมื่อถึงปลายทางแล้วจึงส่งกลับ

- การถามหาแอดเดรสมาสก์ เป็นการให้โฮสต์ถามเซอร์ฟเวอร์เพื่อดูว่าในการทำงานนี้มีแอดเดรสมาสก์หรือ subnet เป็นอย่างไร ลักษณะคำถามที่เกิดขึ้นจึงเกิดจากโฮสต์ถามเราเตอร์ หรือเราเตอร์ถามโฮสต์ หรือโฮสต์ถามโฮสต์

คำถาม Are you alive?

คำถามนี้มีลักษณะการส่งไป ซึ่งเรียกว่า echo และเมื่อปลายทางที่ถามได้รับก็จะ echo ตอบมา รูปแบบของ ICMP เป็นดังรูปที่ 11

ในกรณีที่ type = 8 เป็นคำถามและ type = 0 เป็นคำตอบ โดยการส่งไปจะมีข้อมูลส่งไปด้วย ข้อมูลที่ส่งไปนี้มีขนาดไม่แน่นอนแล้วแต่การกำหนด ตัวตอบกลับมาต้องตอบกลับด้วย ICMP ที่มีขนาดข้อมูลเท่ากัน การมีลำดับเป็นฟิลด์หนึ่งเพื่อให้มีการส่ง ICMP ไปถามหลาย ๆ ตัว และตัวถามก็จะคอยตรวจดูคำตอบว่ามีกลับมาเท่าไร การตรวจสอบนี้จะทำเป็นสถิติได้ว่า เส้นทางที่ไปมีการส่งกลับมาด้วยสถิติอย่างไร

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

type = 8 หรือ 0	Code	check sum
identifier		sequence
ข้อมูล		

รูปที่ 11 รูปแบบคำถามและคำตอบสำหรับ Are you alive?

```
nontri% ping cc2. cpe.ku.ac.th
cc2.cpe.ku.ac.th is alive
nontri%

และ

nontri% ping -s cc2.cpe.ku.ac.th
PING cc2.cpe.ku.ac.th: 56 data bytes
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=0. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=1. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=2. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=3. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=4. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=5. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=6. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=7. time=1. ms
64 bytes from cc2.cpe.ku.ac.th (158.108.33.3) : icmp_seq=8. time=1. ms
^C
--cc2.cpe.ku.ac.th PING Statistics--
9 packets transmitted, 9 packets received, 0% packet loss
round-trip (ms) min/avg/max = 1/1/2
nontri%
```

รูปที่ 12

ลองดูจากคำสั่ง ping อีกครั้ง ดังในรูปที่ 12

จะเห็นได้ว่าคำสั่งแรกส่ง ICMP ไปถามเครื่อง cc2.cpe.ku.ac.th เพื่อให้ตอบว่า alive หรือไม่ แต่ในกรณีหลังมีการให้ตอบกลับมาพร้อมทั้งกำหนดเวลาโดยส่ง 17 แพคเก็ต ข้อมูลขนาด 64 ไบต์ ในฟิลด์ของ identifier เป็นฟิลด์ที่บอกให้รู้ถึง ICMP ตัวใด แต่ลำดับ (sequencer) อาจเปลี่ยนแปลงได้เป็นค่าเพิ่มขึ้นตลอด

สำหรับในการสอบถามเวลามีรูปแบบดังรูปที่ 13

ในการถามเรื่องเวลานี้ type 13 เป็นคำถาม และ type 14 เป็นคำตอบ การถามเรื่องเวลาจะทำให้นำมาคำนวณได้ว่า เวลาที่ใช้ในการส่งไปยังปลายทางและกลับมาอีกครั้งเป็นเท่าไร เวลาของระบบที่ใช้เป็นเวลา GMT โดย ICMP คำถามจะเริ่มใส่เวลาก่อน เมื่อตัวรับรับได้ก็ใส่เวลา ส่งกลับมายังต้นทางรับได้อีกครั้งก็ใส่เวลา ดังนั้นในคำสั่ง ping จึงคำนวณเวลาได้

ICMP คำถามเกี่ยวกับแอดเดรสมาสก์

ขอย้อนไปถึงเรื่องเครือข่าย TCP/IP อีกนิด โดยเฉพาะการแบ่งแยกเป็นเครือข่ายย่อยเพื่อให้เราเตอร์ทำงานได้สะดวกและรวดเร็วขึ้น จึงมีการกำหนดเป็น subnet ด้วยวิธีการมาสก์ การทำงานที่แบ่งแยกเป็นเครือข่ายย่อยจากหมายเลข IP นี้เป็นข้อดี เพราะจะทำให้เราแบ่งแยกออกเป็นโฮสต์ที่ต่ออยู่บนเครือข่ายและแยกฟิลด์ IP ได้ชัดเจน

ในบางครั้งโฮสต์ต้องการอยากรู้ค่าแอดเดรสมาสก์ของตัวเอง หรือกล่าวอีกนัยหนึ่งคือต้องการรู้หมายเลขแอดเดรสของเครือข่ายย่อยที่ตนเองต่ออยู่ วิธีการทำได้ด้วยการถามเซอร์ฟเวอร์ซึ่งก็คือเราเตอร์นั่นเอง

เราเตอร์จะตอบกลับด้วยการให้ข้อมูลแอดเดรสมาสก์มา รูปแบบของ ICMP เป็นดังรูปที่ 14

ในรูปแบบคำถามใช้ type 17 หาก type 18 เป็นคำตอบ และข้อมูลส่วนแอดเดรสมาสก์จะได้รับตอบกลับมา

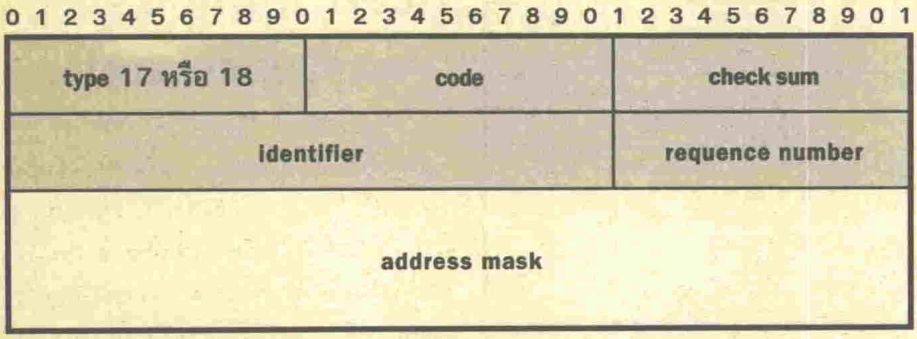
การขอดูสถิติการใช้ ICMP บนโฮสต์

บนเครื่องที่ต่ออยู่กับอินเทอร์เน็ตมีการใช้ ICMP กันอยู่แล้ว และในโฮสต์เองก็มีคำสั่งที่ขอให้ดูสถานะและสถิติการใช้ ICMP ได้ คำสั่งที่ใช้คือ netstat โดยหากต้องการดูสถิติการใช้ให้ใช้พารามิเตอร์- s ดังรูปที่ 15

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type 13 หรือ14	code	check sum
identifier		requence number
originate time stamp		
Receive time stamp		
transmit time stamp		

รูปที่ 13 ICMP ที่สอบถามเรื่องเวลา



รูปที่ 14 คำถามคำตอบของ ICMP เกี่ยวกับแอดเดรสมาสก์

รูปที่ 15

```
nontri% netstat -s | more
ip:
      14687302 total packets received
      0 bad header checksums
      0 with size smaller than minimum
      0 with data size < data length
      0 with header length < data size
      0 with data length < header length
      142 fragments received
      0 fragments dropped (dup or out of spae)
      33 fragments dropped after timeout
      0 pakets forwarded
      0 packets not forwardable
      0 redirects sent
      0 ip input queue drops
icmp:
      4373 calls to icmp_error
      0 errors not generated cuz old message too short
      0 errors not generated cuz old message was icmp
      Output histogram:
            echo reply: 17438
            destination unreachable: 4373
      2 messages with bad code fields
      0 messages < minimum length
      39 bad checksums
      0 messages with bad length
      Input histogram:
            echo reply: 355
            destination unreachable: 4216
            source quench: 15483
            routing redirect: 11
            echo: 17438
            time exceeded: 13952
            parameter problem: 3
      17438 message responses generated
tcp:
      9340476 packets sent
            6698150 data packets (718537031 bytes)
            41395 data packets (6144478 bytes) retransmitted
            2182030 ack-only packets (2049465 delayed)
            304 URG only packets
            6148 window probe packets
            323348 window update packets
            89101 control packets
      14078008 packets received
            670799 acks (for 719186174 bytes)
            70116 duplicate acks
            1 ack for unsent data
            5877431 packets (978776670 bytes) received in-sequence
            44658 completely duplicate packets (10352667 bytes)
            5230 packets with some dup. data (1440417 bytes duped)
            98584 out-of-order packets (28598039 bytes)
            5704 packets (69909 bytes) of data after window
            5615 window probes
            2448072 window update packets                          →
```

รูปที่ 15 (ต่อ)

```
        1747 packets received after close
        7624 discarded for bad checksums
        0 discarded for bad header offset fields
        17 discarded because packet too short
    15888 connection requests
    41379 connection accepts
    52951 connection established (including accepts)
    62862 connection closed (including 4999 drops)
    4079 embryonic connections dropped
    6312548 segment updated rtt (of 6364114 attempts)
    60710 retransmit timeouts
        499 connections dropped by rexmit timeout
        5615 window probes
        2448072 window update packets
        1747 packets received after close
        7624 discarded for bad checksums
        0 discarded for bad header offset filds
        17 discarded because packet too short
    15888 connection requests
    41379 connection accepts
    52951 connections established (including accepts)
    62862 connections closed (including 4999 drops)
    4079 embryonic connections dropped
    6312548 segments updated rtt (of 6364114 attempts)
    60710 retransmit timeouts
        499 connections dropped by rexmit timeout
    11240 persist timeouts
    3139 keepalive timeouts
        318 keepalive probes sent
        2773 connections dropped by keepalive
udp:
    0 incomplete headers
    2 bad data length fields
    0 bad checksums
    288833 socket overflows
nontri%
```

คำสั่ง netstat ในกรณีนี้ให้ข้อมูลทั้ง ip, tcp, udp และ icmp ซึ่งเป็นข้อมูลที่ใช้ในการสื่อสารบนเครือข่าย และหากต้องการดูสถิติการกำหนดเส้นทางใช้คำสั่งดังนี้

```
nontri% netstat -rs | more
routing:
        11 bad routing redirects
        0 dynamically created routes
        0 new gateways due to redirects
        57 destinations found unreachable
        -24073 uses of a wildcard route
nontri%
```

ส่งท้าย

ขบวนการทำงานของเครือข่ายคอมพิวเตอร์ TCP/IP เป็นเรื่องที่มีหลักการและระบบ เครือข่าย TCP/IP จึงเป็นเครือข่ายที่เปิดเผยและเชื่อมต่อถึงกันได้มาก เรียนรู้และเข้าใจได้ ICMP เป็นเพียงโปรโตคอลที่ช่วยระบบให้การทำงานดียิ่งขึ้น ICMP เข้ามาช่วยแก้ปัญหาที่เกิดจากการทำงานปกติของระดับ 3 คือ IP เพื่อว่าการทำงานจะราบเรียบและได้ผลดียิ่งขึ้น

เอกสารอ้างอิง

1. Sidnie Feit "TCP/IP Architecture, Protocols and Implementation" McGraw-hill, Inc., 1993.

รับสมัครด่วน

บริษัทสหอาชีวะอินเตอร์เนชั่นแนล จำกัด เป็นบริษัทฯ นำเข้าอุปกรณ์คอมพิวเตอร์และเป็นตัวแทนขายส่งขายปลีก MONITOR PHILIPS, CD-ROM และ FAX MODEM มีความประสงค์จะรับสมัครผู้มีความกระตือรือร้นและตั้งใจเข้าทำงานกับทางบริษัทฯ จำนวนหลายอัตราดังนี้

1. SALES REPRESENTATIVES
6 อัตรา
- ชาย/หญิง อายุไม่เกิน 30 ปี
- วุฒิ ปวส, ปริญญาตรี ทุกสาขา
- มีประสบการณ์ด้านคอมพิวเตอร์จะพิจารณาเป็นพิเศษ

2. เจ้าหน้าที่ธุรการขาย
1 อัตรา
- หญิง อายุไม่เกิน 27 ปี
- วุฒิ ปวช, ปวส
- สามารถใช้คอมพิวเตอร์ได้จะพิจารณาเป็นพิเศษ

3. เจ้าหน้าที่ช่างบริการ
5 อัตรา
- ชาย อายุไม่เกิน 30 ปี
- วุฒิ ปวช, ปวส สาขาอิเล็กทรอนิกส์
- ถ้ามีประสบการณ์จะพิจารณาเป็นพิเศษ

4. เจ้าหน้าที่ส่งของ
2 อัตรา
- ชาย อายุไม่เกิน 30 ปี
- ไม่จำกัดวุฒิการศึกษา
- มีใบอนุญาติขับขี่รถยนต์
- รู้เส้นทางในกรุงเทพฯ จะพิจารณาเป็นพิเศษ

ผู้สนใจสมัครด้วยตนเอง หรือส่งจดหมายพร้อมหลักฐานการศึกษาและรูปถ่ายมาที่

บริษัท สหอาชีวะอินเตอร์เนชั่นแนล จำกัด
68/2 ถ.สุทธิสารวินิจฉัย ซ.อุดมสุข
ห้วยขวาง กรุงเทพฯ 10310
โทร. 693-0720-4